ІНСТИТУТ ПІДГОТОВКИ КАДРІВ
ДЕРЖАВНОЇ СЛУЖБИ ЗАЙНЯТОСТІ УКРАЇНИ

Мялковський Данило Владиславович

УДК 35:004.056

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ НАДАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

25.00.02 – механізми державного управління

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата наук з державного управління

КИЇВ – 2020

Дисертацією є рукопис.

Робота виконана в Інституті підготовки кадрів державної служби зайнятості України

Науковий керівник – доктор наук з державного управління, професор
заслужений діяч науки і техніки України
СЕМЕНЧЕНКО Андрій Іванович,
Національна академія державного управління при Президентові України,
директор Інституту вищих керівних кадрів.

Офіційні опоненти: доктор наук з державного управління, професор
ГУРКОВСЬКИЙ Володимир Ігорович,
Всеукраїнська громадська організація "Центр досліджень проблем публічного управління",
перший заступник директора;

кандидат наук з державного управління
ОЛЕКСЮК Лілія Віталіївна,
Всеукраїнська асоціація "Інформаційна безпека та інформаційні технології",
Голова громадської організації.

Захист відбудеться *20 серпня 2020 року о 12.00* годині на засіданні спеціалізованої вченої ради Д 26.891.02 Інституту підготовки кадрів державної служби зайнятості України за адресою: 03038, м. Київ, вул. Нововокзальна, 17, к. 201.

З дисертацією можна ознайомитись у бібліотеці Інституту підготовки кадрів державної служби зайнятості України (03038, м. Київ, вул. Нововокзальна, 17).

Автореферат розісланий *16 липня 2020 року.*

Вчений секретар
спеціалізованої вченої ради М. З. Масик

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження обумовлена зростанням кількості електронних послуг, які використовують інформацію різного ступеня обмеження доступу, їх широким проникненням та впливом на життєдіяльність громадянина, суспільства та держави, розвитком інформаційно-комунікаційних технологій (ІКТ), постійним зростанням вартості інформації як активу, удосконаленням існуючих та розробленням нових способів реалізації загроз для безпеки інформації на всіх етапах її життєвого циклу, розробленням та впровадженням додаткових механізмів, спрямованих на підвищення якості електронних послуг та безпеки інформації при їх наданні. Забезпечення безпеки інформації, тобто збереження її конфіденційності, цілісності, доступності, застосовності, авторства та спостережності під час її оброблення в існуючих і новостворених системах електронних послуг стає визначальним чинником довіри до результатів їх надання. Одним із механізмів забезпечення такої довіри є надання електронних послуг з використанням нормативно врегульованих електронних довірчих послуг.

Прийшовши на зміну Законам України “Про електронний цифровий підпис”, “Про електронні довірчі послуги”, та низки розроблених на їх виконання підзаконних нормативно-правових актів, визначено норми, спрямовані на імплементацію в Україні Регламенту ЄС “Про електронну ідентифікацію та електронні довірчі послуги”. Цим Законом, як і вказаним Регламентом, визначено перелік базових електронних послуг, надання яких за визначеними цими актами правилами забезпечує підвищений (для електронних довірчих послуг) та високий (для кваліфікованих електронних довірчих послуг) рівень запевнень в їх безпечності, а також запроваджено низку новацій. Такими новаціями, зокрема, є: застосування міжнародних стандартів та практик щодо безпеки інформації насамперед європейських, які, на відміну від українського законодавства у сфері захисту інформації, більше відповідають сучасним безпековим вимогам, постійно оновлюються; вирішення завдання технологічної сумісності (інтероперабельності) електронних підписів та їх сертифікатів на рівні ЄС, які охоплюють ширший спектр питань стандартизації та оцінки відповідності у сфері електронної ідентифікації та електронних довірчих послуг тощо.

Українське законодавство у сфері захисту інформації ґрунтується на Законах України “Про інформацію” та “Про захист інформації в інформаційно-телекомунікаційних системах”. Ними визначено базову термінологію та з’ясовано, що захист інформації є одним із основних видів інформаційної діяльності у сфері державної політики і регулювання, що забезпечує її в таких галузях: електронне врядування, надання електронних послуг, електронна ідентифікація та електронні довірчі послуги, державний контроль за міжнародними передачами товарів військового призначення та подвійного використання, кібербезпека, технічне регулювання, наукова та науково-технічна експертиза.

Законодавством у сфері захисту інформації, базис якого формувався й увібрав майже всі передові світові практики на межі XX-XXI століть, врегульовано завдання та обов’язки суб’єктів, процедури, визначено вимоги з захисту інформації, порядок та оцінку їх виконання при розробленні, впровадженні та використанні засобів,

механізмів та систем захисту інформації.

У зв'язку з цим важливим є дослідження ефективності державного регулювання у сфері захисту інформації та його спроможності забезпечити належний рівень безпеки як процесів електронної ідентифікації та електронних довірчих послуг, так й інформації, що використовується при наданні електронних послуг взагалі, яка буде визначальним фактором успіху розпочатих реформ та переходу до цифрової економіки та суспільства.

Аналіз стану сфери захисту інформації в Україні доводить наявність законодавчої бази у сфері захисту інформації, відповідної організаційно-технічної інфраструктури, розвинених національних криптографічних шкіл, які розробляють сучасні та квантово-стійкі криптографічні алгоритми та протоколи, достатньо високого рівня стандартизації криптографічних механізмів як національної розробки, так і визначених міжнародними стандартами, підприємств-розробників та виробників, що випускають на ринок засоби захисту інформації різного ступеня обмеження доступу, зокрема засоби генерації ключів, накладання/перевірки електронного підпису, стабільно високого попиту на вітчизняну криптографічну продукцію, потребу в підтвердженні відповідності такої продукції та процесів їх створення міжнародним вимогам, взаємному з іншими країнами та їх об'єднаннями визнанні сертифікатів відповідності.

За кордоном проблематику безпеки інформації з впровадження електронних послуг з використанням електронних підписів досліджували Алі Ал-Зубіассам (Ali Al-Zubiassam), Ал-Травнех (Al-Trawneh), Інду Ніранйан (Indu Niranjan), А. Сеетхараман (A. Seetharaman), Веена Ядхау (Veena Jadhav), Аріндам Банер'є (Arindam Banerjee), Томас Гросс (Thomas Gross), Стефан Кренн (Stephan Krenn), Кai Самелін (Kai Samelin), Дієтер Соммер (Dieter Sommer), Генріх С. Пьольс (Henrich C. Pöhls) та інші.

В їх роботах досліджувались проблематика реалізації кваліфікованих підписів, електронних договорів та транзакцій в окремих країнах, моделі управління ризиками задля безпеки інформації при застосуванні різних електронних підписів, схеми, графи електронних підписів для доведення неспростовності дій, проблематика забезпечення цілісності та конфіденційності підписаних електронним підписом даних, впровадження схем повторного електронного підпису для підвищення конфіденційності.

Багато українських учених присвятили свої роботи вирішенню завдання створення національної інфраструктури відкритих ключів та її відповідності міжнародним стандартам: І.Д. Горбенко, Ю.І. Горбенко, Н.А. Літвінова, О.В. Літвінов, І.В. Кліменко, О.В. Костенко, Є.В. Брошеван, О.В. Потій, А.В. Гречко, А.О. Мелащенко, С.В. Таран, Н.В. Білоцерковець, О.В. Голіна, В.В. Ліпінський, О.І. Братков, Ю.А. Кірпічніков, Ю.В. Кондратенко, Г.В. Руденська, С. І. Васюхно, А.І. Семенченко, А.В. Журавльов, Л.В. Олексюк, С.А. Чукут та інші.

У цих роботах проведений аналіз стану, сутності та сучасних проблем електронного підпису, питання, що стримують широке його застосування з огляду на особливості національного регулювання цієї сфери, можливі шляхи подальшого розвитку технологічної інфраструктури надання електронних послуг, захищеність персональних даних, даних реєстрів та електронної ідентифікації нотаріусів.

Досліджувалась методологія організації роботи державного органу задля впровадження електронних державних послуг, порівняльний аналіз практик Європейського Союзу щодо надання електронних послуг, США, Канади та країн Азії щодо впровадження електронних державних послуг, аналіз транскордонної взаємодії, впровадження електронної довірчої послуги – гарантованої доставки, її технічні та організаційні особливості, імплементація електронних довірчих послуг шляхом впровадження програмної бібліотеки з відкритим вихідним кодом Digital Signature Service (DSS), державне регулювання діяльності провайдерів некваліфікованих електронних довірчих послуг, їх права та обов'язки, вдосконалення нормативно-правового регулювання створення та впровадження комплексних систем захисту інформації в інформаційних системах з використанням положень стандартів НАТО, державного управління у сфері електронного врядування тощо.

Однак, не зважаючи на значну кількість підходів до вирішення проблеми забезпеченням безпеки надання електронних довірчих послуг, вона залишилася актуальною не тільки для України, але й для багатьох країн світу та їх об’єднань як у теоретичному, так і в практичному плані.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційна робота проводилася в межах науково-дослідних робіт Інституту підготовки кадрів державної служби зайнятості України за темою кафедри публічного управління та адміністрування – “Модернізація та підвищення ефективності публічного управління у сфері зайнятості в Україні в контексті євроінтеграції” (2018 – 2023 рр.) (ДР № ДЄ №01118 U 003561), в яких автором проведено комплексне дослідження механізмів державного регулювання забезпеченням безпеки надання електронних довірчих послуг та розроблено практичні рекомендації щодо вдосконалення діяльності органів влади в цій сфері.

Мета і завдання дослідження. Метою дисертаційного дослідження є обґрунтування теоретико-методологічних засад та розроблення практичних рекомендацій щодо удосконалення механізмів державного регулювання забезпеченням безпеки надання електронних довірчих послуг.

Для досягнення поставленої мети було визначено такі завдання:

– розробити пропозиції щодо удосконалення категорійно-понятійного апарату за результатами аналізу та узагальнення існуючих теоретико-методологічних напрацювань з проблеми державного регулювання у сфері захисту інформації, електронної ідентифікації та електронних довірчих послуг;

– узагальнити досвід провідних країн світу та їх об’єднань, насамперед НАТО та Європейського Союзу, та визначити тенденції розвитку їх систем державного регулювання забезпеченням безпеки надання електронних довірчих послуг;

– оцінити існуючі механізми взаємодії складових системи захисту інформації для потреб забезпечення безпеки надання електронних довірчих послуг та розробити пропозиції щодо її осучаснення та подальшого розвитку;

– проаналізувати підходи щодо удосконалення нормативно-правових та організаційно-технічних механізмів державного регулювання у сферах захисту інформації й електронної ідентифікації та електронних довірчих послуг;

– визначити мотиваційні механізми запровадження систем для підвищення рівня безпеки інформації при наданні електронних послуг;

– надати пропозиції щодо популяризації в суспільстві правил дотримання безпеки інформації при отриманні електронних довірчих послуг;

– удосконалити механізм моніторингу стану безпеки надання електронних довірчих послуг.

– запропонувати рекомендації державним органам щодо підвищення якості та ефективності надання електронних послуг з використанням електронних довірчих послуг.

Об'єкт дослідження – державна політика у сфері захисту інформації, електронної ідентифікації та електронних довірчих послуг.

Предмет дослідження – механізми державного регулювання забезпеченням безпеки надання електронних довірчих послуг.

Методи дослідження. Для виконання поставлених завдань дослідження використано загальнонаукові та спеціальні методи:

– діалектичний – при виявленні та дослідженні взаємозв'язків між суб'єктами/об'єктами-учасниками процесів надання електронних довірчих послуг, визначенні ризиків, що впливатимуть на їх діяльність та безпеку функціонування, встановлення ступеня впливу цих ризиків на попередньо визначену оцінку довіри до електронних довірчих послуг, також у процесі розроблення нормативно-правових та організаційно-технічних механізмів забезпечення безпеки електронних довірчих послуг;

– емпіричні (спостереження, порівняння, вимірювання) – при зборі інформації в процесі аналізу норм національних законодавств щодо даних, необхідних для надання/отримання електронних довірчих послуг відповідно до таких норм, статистичних даних про кількість та динаміку їх змін щодо електронних довірчих послуг, способів їх отримання, затребуваності, термінів чинності та використання їх результатів, кількості інформаційно-телекомунікаційних систем, залучених для надання електронних довірчих послуг, підтвердження відповідності таких систем вимогам безпеки, кількості постачальників обладнання й прикладного програмного забезпечення та його критичних елементів для отримувачів та надавачів електронних послуг, рівні довіри до обладнання ІТС та загального програмного забезпечення в середовищі якого застосовується прикладне програмне забезпечення, безпеки програмного забезпечення телекомунікаційного обладнання та інші дані;

– історичний – для дослідження виникнення механізмів регулювання захистом інформації;

– системно-аналітичний метод – для дослідження процесів формування нормативно-правового і організаційного механізмів управління процесами захисту інформації, вибудовування ланцюгів процесів створення, дослідження, оцінки відповідності, контролю тощо, доведена безпека кожного елементу з яких є чинником для інтегрованого показника довіри до електронних послуг;

– аналіз тенденцій – для відстеження динаміки зміни та обсягів надання електронних довірчих послуг з використанням електронного підпису;

– узагальнюючий і порівняльний – для оцінки діючого механізму державного

регулювання захистом інформації та дослідженню можливостей апробації міжнародного досвіду;

– суб'єктно-об'єктний – для удосконалення механізму державного регулювання захистом інформації;

– методи синтезу та узагальнення – для формування пропозицій щодо удосконалення системи державного регулювання захистом інформації в Україні, розробленні пропозицій щодо осучаснення системи захисту та безпеки інформації в умовах все більш широкого впровадження продуктів ІКТ у повсякденну діяльність громадянина, суспільства та держави.

Методологічною базою дослідження є наукові праці вітчизняних і зарубіжних учених, зокрема офіційні публікації міжнародних організацій. Інформаційну та емпіричну базу дослідження сформували нормативні документи органів державної та регіональної влади, статистичні та соціологічні дані, матеріали, опубліковані в періодичних виданнях та мережі Інтернет.

Наукова новизна одержаних результатів полягає в обґрунтуванні, поглибленні та розробці теоретико-методологічних засад та практичних рекомендацій щодо розвитку механізмів державного управління забезпеченням довіри до електронних послуг.

У результаті проведеного дослідження сформульовано низку положень, що мають важливе теоретичне і практичне значення, а саме:

уперше:

– розроблено комплексний механізм державного регулювання безпекою надання електронних довірчих послуг, що включає сукупність взаємно пов'язаних організаційних, правових, мотиваційних, моніторингових, організаційно-технічних механізмів, кожний з яких запропоновано реалізувати шляхом внесення змін у національне законодавство з урахуванням міжнародного досвіду Європейського Союзу, НАТО та особливостей розвитку України, що сприятиме підвищенню рівня його ефективності, так і рівня інтероперабельності при транскордонній взаємодії з країнами ЄС та НАТО;

– здійснено порівняльний аналіз низки базових правових та організаційних механізмів ЄС та НАТО щодо процедур оцінки відповідності та акредитації з безпеки чутливої інформації та інформаційно-телекомунікаційних систем, що її обробляють, зберігають та передають, стосовно національного законодавства в цій сфері, визначено їх переваги та основні умови їх успішного впровадження в Україні;

– за результатами аналізу інституційного механізму НАТО акредитації з безпеки інформаційно-телекомунікаційних систем, які зберігають та передають інформацію НАТО з обмеженим доступом, обґрунтовано інституціональну готовність основних суб'єктів сектору безпеки і оборони України до проведення акредитації національних інформаційно-телекомунікаційних систем, а також запропоновано поетапне впровадження комплексу організаційно-правових, комунікативних та інформаційно-аналітичних заходів з такої акредитації в Україні;

удосконалено:

– визначення основоположних понять для осучаснення термінології у сфері захисту інформації, а саме "ідентифікація", "доказування ідентифікації"

“автентифікація”, “рівень запевнень”, “система управління безпекою інформації”, “безпека надання електронних довірчих послуг” тощо, які, на відміну від існуючих, більшою мірою відповідають сутності, особливостям та тенденціям розвитку сфери електронної ідентифікації та електронних довірчих послуг;

– правовий механізм державного регулювання безпекою надання електронних довірчих послуг шляхом внесення змін до Закону України “Про захист інформації в інформаційно-телекомунікаційних системах”, який, на відміну від існуючого, забезпечить зміну парадигми цієї сфери: перехід від “захисту інформації”, як процесу надання набору послуг безпеки, до “безпеки інформації”, як її стану, а також внесенням змін до Закону України “Про електронні довірчі послуги”, а саме щодо запровадження процедури регулювання електронної ідентифікації та розбудови для цього відповідних інституціональних спроможностей, запровадження процедури регулювання діяльності некваліфікованих провайдерів електронних довірчих послуг, зокрема щодо забезпечення безпеки інформації під час надання ними електронних довірчих послуг, встановлення вимог до них та відповідальності за їх порушення;

– організаційно-технічний механізм державного регулювання безпекою надання електронних довірчих послуг шляхом застосування міжнародних стандартів з оцінки відповідності, вимог до суб’єктів, що її здійснюють, з метою наближення національної системи оцінки відповідності до міжнародної;

набули подальшого розвитку:

– дослідження основних тенденцій розвитку у сфері електронної ідентифікації та електронних довірчих послуг у країнах ЄС, основні проблеми в цій сфері в Україні, що дозволило підвищити рівень обґрунтованості пропозицій з модернізації механізмів державного регулювання безпекою електронних довірчих послуг, а також посилити спроможність систем, що їх надають, адекватно протистояти як відомим, так і новим викликам та загрозам для безпеки інформації;

– обґрунтування необхідності перегляду цілей та завдань міжнародної технічної допомоги у сфері захисту систем надання електронних послуг, а саме: поступова відмова від отримання матеріально-технічних засобів у сфері ІКТ, які постійно морально та фізично застарівають швидше, ніж всі інші активи, зосередившись на отриманні та постійному вдосконаленні необхідних для цифровізації знань та цифрових навичок публічних службовців та громадян, запровадження прозорих та зрозумілих підходів до забезпечення безпеки чутливої для громадян, суспільства та держави інформації, а також необхідність визначення в Україні своїх національних пріоритетів цифрової трансформації, адаптованими з аналогічними цілями в ЄС.

Практичне значення одержаних результатів полягає в тому, що теоретичні положення, висновки та рекомендації, розроблені автором і запропоновані в дисертації, вже використані та можуть бути в подальшому реалізовані для вдосконалення комплексного механізму державного управління забезпеченням безпеки надання електронних довірчих послуг, що сприятиме розвитку екосистеми безпеки надання електронних послуг, зокрема, електронних довірчих послуг, зрілості підприємств, установ і організацій у цій сфері, залученню інвестицій,

підвищенню якості та ефективності електронних послуг, покращить довіру громадян до їх результатів.

Наукові висновки й теоретичні положення дисертаційної роботи фактично доведені до рівня конкретних пропозицій і практичних рекомендацій для використання в галузі державного управління. Зокрема, результати дослідження були використані в практичній діяльності Державного агентства з питань електронного урядування України (довідка про впровадження № 1/22-3-1352 від 21.06.2019), Державної служби спеціального зв'язку та захисту інформації України (довідка про впровадження № 04/02/02-1979 від 22.07.2019), Києво-Святошинської районної державної адміністрації Київської області (довідка № 07-34/2616 від 04.09.2019), Державного підприємства "Національні інформаційні системи" (довідка про впровадження № 2987/12.1-06 від 31.07.2019).

Особистий внесок здобувача. Дисертаційна робота є завершеним самостійним науковим дослідженням автора, що містить теоретичні положення, практичні розробки, висновки та пропозиції, які одержано й сформульовано особисто автором, та які в комплексі дають можливість вирішення важливого наукового завдання щодо вдосконалення та реалізації комплексного механізму державного регулювання забезпеченням безпеки надання електронних довірчих послуг в Україні.

Апробація результатів дослідження. Основні положення дисертаційного дослідження були презентовані та обговорені на міжнародних і всеукраїнських науково-практичних конференціях, зокрема: "Науково-практичне забезпечення децентралізації надання послуг в об'єднаних територіальних громадах" (м. Київ, 18 квітня 2018 р.); "Освітньо-наукове забезпечення складових сектору безпеки і оборони України" (м. Хмельницький, 15 листопада 2018 р.), "Сучасні інформаційні технології та кібербезпека" (м. Київ, 15-16 листопада 2018 р.); "Побудова інформаційного суспільства: ресурси і технології" (м. Київ, 19-20 вересня 2019 р.); "Прикладні системи та технології в інформаційному суспільстві" (м. Київ, 30 вересня 2019 р.); "Організаційно-управлінські та психологічні аспекти сучасного ринку праці України" (м. Київ, 29 жовтня 2019 р.); "Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання" (м. Київ, 19-20 листопада 2019 року).

Публікації. Основні положення та отримані наукові результати дисертаційного дослідження відображено в 19 наукових працях, з яких: 6 статей – опубліковано у вітчизняних наукових фахових виданнях з державного управління, 1 стаття – у зарубіжному спеціалізованому виданні, 7 тез доповідей – у збірниках матеріалів науково-практичних заходів, 5 праць, які додатково відображають наукові результати дисертації.

Структура та обсяг дисертації. Дисертація складається з переліку умовних позначень, вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 284 сторінок. Обсяг основного тексту – 211 сторінок. Робота налічує 40 рисунків, 10 таблиць. Список використаних джерел налічує 226 найменувань на 29 сторінках.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** обґрунтовано вибір, актуальність і стан розробки теми дисертаційної роботи, подано її загальну характеристику, вказано на зв'язок дисертації з науково-дослідними роботами, визначено мету, завдання, об'єкт, предмет, охарактеризовано методологічну базу, наукову новизну та практичну значущість одержаних результатів, наведено дані щодо апробації та опублікування результатів дослідження.

У першому розділі – "*Теоретико-методологічні засади механізмів державного управління захистом інформації для забезпечення безпеки при електронній ідентифікації та надання електронних довірчих послуг"* – розкрито сутність, основні поняття, терміни щодо захисту інформації, механізми безпеки, які застосовуються для забезпечення безпеки надання електронних послуг, та їх взаємний зв'язок. У процесі аналізу предметної області встановлена відсутність та запропоновано авторське визначення поняття "безпека надання електронних довірчих послуг", розкритий зв'язок понять "захист інформації", "кібербезпека", "безпека інформації" та "інформаційна безпека".

При аналізі типових законів, розроблених ООН (UNCITRAL), "Про електронну торгівлю" та "Про електронні підписи", встановлено, що провідні країни світу (Канада, КНР, Республіка Корея, США, Турецька Республіка, країни-члени ЄС) широко застосовують впроваджені в цих законах моделі, що забезпечило як певну схожість національних законодавств у сфері електронних підписів, так і однаковість проблем, основною з яких є забезпечення технологічної сумісності (інтероперабельності). Основними в проблематиці сумісності є застосування однакових криптографічних алгоритмів електронного підпису та гешування, формати даних електронних підписів та їх сертифікатів відкритих ключів електронних підписів, які не оминули й Україну. У країнах ЄС криптографічна сумісність забезпечена шляхом затвердження Єврокомісією документа із стандартизації (Мандат 460) та відповідного стандарту ETSI TS 119 312 з визначеними парами криптографічних алгоритмів електронного підпису та гешування.

За результатами аналізу впровадження електронних послуг в Україні визначено його стан за різними міжнародними індексами: розвитку електронного врядування, глобального та національного індексів кібербезпеки, розвитку ІКТ. З'ясовано проблеми з формуванням та реалізацією ефективної державної політики, зокрема у сферах: розвитку електронного врядування, забезпечення безпеки інформації при наданні електронних послуг та електронних довірчих послуг, вирішення завдань безпеки інформації при використанні ІКТ, низьке розуміння цілей безпеки інформації при впровадженні інформаційних та інформаційно-телекомунікаційних систем для надання електронних послуг.

Здійснено ретроспективний аналіз становлення та розвитку інфраструктури надання електронних довірчих послуг в Україні та статистичних даних динаміки кількості надавачів електронних довірчих послуг та їх використання в різних електронних сервісах. Алгоритмічна сумісність у середині України була забезпечена застосовністю на початку розбудови інфраструктури електронних підписів лише

національного алгоритму електронного підпису, а сумісність при міжнародній взаємодії – впровадженням лише з 2017 року криптоалгоритмів, визначених гармонізованим з міжнародним національним стандартом ДСТУ ETSI TS 119 312: 2015.

Проведено аналіз етимологічної моделі у сфері електронної ідентифікації в Україні, за результатами якого встановлено часткову відповідність визначень термінів, відсутність термінів "ідентичність" та "доказування ідентичності", які потребують нормативного визначення. Досліджено, що інфраструктура відкритих ключів електронного підпису стає критичною інформаційною інфраструктурою. Безпека її функціонування має на сьогодні розглядатись не тільки в площині Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", а й Закону України "Про основні засади забезпечення кібербезпеки України".

У другому розділі – *"Механізми державного регулювання забезпеченням безпеки надання електронних довірчих послуг"* – розкривається відмінність базових правових механізмів ЄС щодо забезпечення надання електронних довірчих послуг відносно національного законодавства в цій сфері, які впроваджені в Україні частково. З метою підвищення рівня забезпечення безпеки надання електронних довірчих послуг, а також їх більшої застосовності, автором запропоновано внесення низки змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", який, на відміну від існуючого, забезпечить зміну парадигми цієї сфери: перехід від "захисту інформації", як процесу надання набору послуг безпеки, до "безпеки інформації", як її стану, а також до Закону України "Про електронні довірчі послуги", а саме щодо запровадження регулювання електронної ідентифікації, як загальнодержавного процесу, та необхідності розбудови для цього інституціональних спроможностей, запровадження регулювання діяльності некваліфікованих провайдерів електронних довірчих послуг, зокрема щодо забезпечення безпеки надання ними електронних довірчих послуг, та удосконалення діяльності контролюючого органу.

За результатами аналізу цілей та завдань міжнародної технічної допомоги, визначено необхідність суттєвої модернізації підходу до їх визначення: замість отримання матеріально-технічних засобів у сфері ІТ, які застарівають скоріше, ніж всі інші активи, отримувати та постійно вдосконалювати необхідні для цифрової економіки знання та навички широким загалом населення, запроваджувати прозорі та зрозумілі підходи до забезпечення безпеки чутливої для громадян, суспільства та держави інформації, а також необхідність визначення в Україні своїх пріоритетів у переході до цифрової економіки, які мають співвідноситися з аналогічними цілями в ЄС.

Досліджено правовий механізм забезпечення взаємного визнання електронної ідентифікації та її схем, електронних довірчих послуг та результатів оцінки відповідності надавачів електронних довірчих послуг шляхом підготовки міжнародних договорів України з ЄС (країнами-членами) у цій сфері.

Здійснено порівняльний аналіз організаційно-правових механізмів державного управління проведенням акредитації комунікаційно-інформаційних систем (КІС) для обміну інформацією з обмеженим доступом в Україні та НАТО, подано оцінку рівня їх інтероперабельності, на основі якої обґрунтовано узагальнюючий висновок

щодо наявності в Україні засобів КЗІ для різних ступенів обмеження доступу до інформації, які відповідають національному законодавству та політиці безпеки України та можуть бути, після визначення їх конкретних типів, запропоновані стороні НАТО для погодження оброблення інформації з обмеженим доступом в Україні.

Розглянуто правовий механізм забезпечення прийняття Адміністрацією Держспецзв'язку рішення, про проведені акредитації конкретної КІС, яка відповідає законодавству України, про оброблення (пересилання, зберігання) в ній інформації з грифом обмеження доступу NATO "CONFIDENTIAL" та NATO "RESTRICTED", а також для інформації NATO "SECRET".

Проведено аналіз інституціональної готовності суб'єктів сектору безпеки і оборони України до організації та виконання заходів з акредитації КІС для обміну інформацією з обмеженим доступом з НАТО, насамперед Мінооборони та Генерального штабу Збройних Сил України, Національної гвардії України, МВС, Держприкордонслужби та Держспецзв'язку та інших.

Здійснено ретроспективний аналіз формування нормативно-правової бази системи НАТО PKI (NPKI) та запропоновано авторську етапізацію її розвитку за критерієм підтвердження відповідності засобів та процесів, а саме: створення рамкового середовища та інфраструктури, використання під час дослідної експлуатації формально недозволених через незавершеність процедур тестування засобів електронного підпису (1998 – 2006 рр.), розвиток інфраструктури, засобів та сервісів з використанням NPKI (2006 – 2013 рр.), розвиток інфраструктури та впровадження проєкту використання сервісів NPKI для всеохоплюючого задоволення інформаційних потреб користувачів Штаб-квартири НАТО та країн-членів (з 2013 р.).

Проведено порівняльний аналіз принципів забезпечення безпеки інформації в NPKI з інфраструктурою електронних підписів, відбудованої в ЄС згідно з Регламентом ЄС з електронної ідентифікації та електронних довірчих послуг, який показав їх взаємну узгодженість.

У третьому розділі – *"Рекомендації державним органам щодо удосконалення механізмів державного регулювання забезпеченням безпеки електронних довірчих послуг"* – встановлено, що недостатня розвиненість на цей час в Україні інфраструктури оцінки відповідності та відсутність акредитованих в Україні органів з оцінки відповідності не дає можливості для проведення відповідних оцінок надавачів електронних довірчих послуг, а також засобів їх надання для взаємного поширення цифрового простору довіри між ЄС та Україною.

Проведено аналіз державного технічного регулювання для визначення можливості взаємного визнання в Україні результатів оцінки відповідності, здійсненої органами з оцінки в європейських країнах шляхом підписання відповідного міжнародного договору України.

Досліджено проблеми забезпечення технологічної сумісності електронних підписів та засобів кваліфікованого електронного підпису в електронних сервісах в Україні та напрямки її забезпечення. Зосереджено увагу на застосуванні спеціалізованих програм забезпечення взаємодії програмного та апаратного забезпечення (крипто бібліотек) різних виробників засобів кваліфікованого

електронного підпису для забезпечення широкого застосування електронних довірчих послуг в електронних сервісах. Стимулювання участі у проєктах щодо державних систем надання електронних послуг з використанням електронних довірчих послуг можливо вирішувати в межах державно-приватного партнерства та запровадження мотиваційних механізмів державного управління забезпеченням безпеки їх надання. Їх реалізація має, з одного боку, виключити безпосередній контакт регулятора у сфері захисту інформації з бізнес-структурами, з іншого – надати поштовх у розвитку інфраструктури захисту інформації, що стане підґрунтям для вибудовування інфраструктури нового зразка – безпеки інформації. Проаналізовано причини виникнення, існуючий стан справ та розроблено пропозиції щодо розвитку сфери підготовки кадрів у галузі захисту інформації та її безпеки.

Охарактеризовано основні передумови та чинники, що впливають на систему захисту інформації як системоутворюючого елемента забезпечення її безпеки та довіри до електронних довірчих послуг, а також на підставі проведеного аналізу визначено шляхи реформування цієї галузі та розроблено пропозиції до змін законодавства, які забезпечують трансформацію самої парадигми функціонування системи: від контролю за процесами захисту інформації до оцінки стану її безпеки. Автором запропоновано комплексне рішення щодо внесення змін або розроблення нових законодавчих актів, що забезпечить осучаснення підходів до безпеки інформації.

Розроблено комплекс рекомендацій Раді національної безпеки і оборони України, Держспецзв'язку, Міноборони та Генеральному штабу Збройних Сил України, Мінекономрозвитку, Міносвіти, МЗС, Мінцифри та іншим міністерствам, центральним органам виконавчої влади щодо дієвих кроків з удосконалення галузі захисту інформації та її розвитку в напрямку забезпечення безпеки інформації, а також розвитку власних спроможностей у протидії загрозам інформації, забезпеченні її безпеки та довіри до електронних послуг, що ними надаються.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне наукове завдання, яке полягає у теоретико-методологічному обґрунтуванні розроблення комплексного механізму державного регулювання забезпеченням безпеки надання електронних довірчих послуг та розробленні практичних рекомендацій щодо вдосконалення процедур і технологій його реалізації в сучасних умовах суспільного розвитку. Результати, отримані в процесі дослідження, підтверджують досягнення поставленої мети й вирішення завдань, дають підстави сформулювати такі висновки і практичні рекомендації.

1. На основі проведеного аналізу з'ясовано, що існують розбіжності в термінології та визначенні понять "ідентифікація", "доказування ідентифікації", "автентифікація", "рівень запевнень", "система управління безпекою інформації" тощо відносно застосованих у міжнародних, зокрема, європейських стандартах, що ускладнює реалізацію відповідних технічних механізмів в ІТС та можливість довести досягнутий рівень безпеки при їх застосуванні. Запропоновано авторське

визначення терміну “безпека надання електронної довірчої послуги” як інтегрований показник, який визначається доведеним рівнем запевнень у правильності встановлених сценаріїв, способів, суб’єктів та обраних засобів надання електронної довірчої послуги та можливості системи, що надає електронну довірчу послугу, постійно бути в стані відповідності новим загрозам безпеці інформації та цій системі. У випадку, якщо такий рівень доведений, то електронна довірча послуга стає кваліфікованою електронною довірчою послугою.

Термінологічна база у сфері захисту інформації та довірчих послуг вимагає подальшого удосконалення з урахуванням досвіду розроблення національних стандартів, гармонізованих із стандартами ISO/IEC та ETSI, приведення у відповідність до регламентів та директив у сфері електронної ідентифікації та електронних довірчих послуг, безпеки мереж та інформаційних систем, сертифікації з кібербезпеки, оскільки це безпосередньо впливає на результати оцінки відповідності українських інфраструктур вимогам законодавчих актів ЄС у цій сфері.

2. Зазначено, що в національних законодавствах країн світу широко застосовуються розроблені та прийняті ООН типові закони про електронну комерцію та електронні підписи з керівництвами про введення їх в дію. Переважна більшість національних законодавств мають незначні відмінності порівняно з зазначеними законами UNCITRAL та застосовують однакові базові міжнародні стандарти, проте їх практична реалізація має відмінності. Наслідком таких відмінностей є проблема відсутності інтероперабельності (технологічної сумісності) електронних цифрових підписів не тільки на міжнародному рівні, а й в середині країн, яка полягає в різних застосованих криптографічних алгоритмах ЕЦП та гешуванні, форматів як самих ЕЦП, так і сертифікатів ключів ЕЦП, інформаційних повідомлень тощо.

Обрання для використання конкретних криптографічних методів здійснюється в національних законодавствах з урахуванням наявності/відсутності національних криптоалгоритмів, їх стійкості, визначеної з урахуванням постійного розвитку спроможностей потенційного порушника, за відсутності національних рішень з урахуванням поширеності та застосовності алгоритмів у світі, простоти їх реалізації у відповідних програмних та апаратних платформах, вибагливості до обчислювальної потужності до апаратних платформ, а також спроможності нормативно забезпечити дотримання правил їх застосування, що визначає надійність та має виключну роль у забезпеченні безпеки сучасних комунікацій, безперервності та довіри до сервісів тощо.

Вітчизняні криптографічні алгоритми можуть бути запропоновані для широкого застосування не тільки в Україні, а й у світі, оскільки вони враховують розвиток систем квантових обчислень та вже зараз алгоритми блочного та потокового шифрування мають високу квантову криптографічну стійкість.

Європейський Союз та його країни-члени пройшли шлях від створення національних законодавств до пан’європейського регулювання застосовності електронних підписів. Реалізована в регуляції ЄС вимога щодо недопущення дискримінації національних рішень забезпечила реалізацію можливості перевіряння електронних підписів та сертифікатів ключів таких підписів, випущених у країнах-

членах ЄС до впровадження загальноєвропейського регулювання цієї сфери. З іншої сторони, проблема забезпечення інтероперабельності змусила європейські органи зі стандартизації розробити та впровадити стандарти. Так, для забезпечення криптографічної сумісності, наприклад, до відповідних технічних специфікацій увійшли всі можливі та застосовані в країнах ЄС комбінації криптографічних алгоритмів електронного підпису та гешування. Такий підхід забезпечив інтероперабельність на рівні ЄС національних інфраструктур його країн-членів. Це є цінний досвід, яким доцільно користуватися країнам, маючим на меті транскордонне визнання з ЄС електронних підписів, серед яких є і наша держава.

3. Обґрунтовано, що Україна має високі показники розвитку електронного врядування, впровадження електронних послуг у повсякденне життя громадян, суспільства і держави. На сьогодні наявні більше 150 електронних послуг із застосуванням електронного підпису та майже дев'ятимільйонна аудиторія власників електронних підписів. З огляду на це можна зазначити, що інфраструктура відкритих ключів електронного підпису стає критичною інформаційною інфраструктурою. Безпека її функціонування має розглядатись не тільки в площині Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", а й Закону України "Про основні засади забезпечення кібербезпеки України".

4. Удосконалено правовий механізм державного регулювання безпекою надання електронних довірчих послуг шляхом внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", який, на відміну від існуючого, забезпечить зміну парадигми цієї сфери: перехід від "захисту інформації" як процесу надання набору послуг безпеки до "безпеки інформації" як її стану. З метою підвищення рівня безпеки електронних довірчих послуг, а також їх більшої застосовності, автором запропоновано внесення низки змін до Закону України "Про електронні довірчі послуги", а саме щодо запровадження регулювання електронної ідентифікації як загально державного процесу, та необхідності розбудови для цього інституціональних спроможностей, запровадження регулювання діяльності некваліфікованих провайдерів електронних довірчих послуг, зокрема щодо забезпечення безпеки інформації під час надання ними електронних довірчих послуг, відповідальності за її порушення та удосконалення діяльності контролюючого органу.

Базові правові механізми ЄС щодо забезпечення безпеки та довіри до електронних послуг мають перевагу стосовно національного законодавства в цій сфері та впроваджені в Україні частково.

Прийняття нового законодавства щодо електронних довірчих послуг неповною мірою забезпечило імплементацію європейських новацій у цій сфері. Під механізмом забезпечення довіри до електронних послуг, хоча і визначено в законі можливість застосування моделі забезпечення безпеки інформації, проте він передбачає застосовність застарілої моделі – оцінки відповідності комплексних систем захисту інформації у межах державної експертизи у сфері захисту інформації. Це може розглядатися в умовах перехідного періоду (до набуття чинності всіх норм закону), проте не сприйматиметься так, як його розуміють в Україні при подальших кроках у нормативному закріпленні взаємного визнання з

ЄС електронних підписів та довірчих послуг. Це вимагатиме впровадження оцінки відповідності систем забезпечення безпеки інформації за правилами ЄС.

Наголошено, що процедура первинної ідентифікації в системі забезпечення довіри електронних послуг, яка здійснюється за умови особистої присутності майбутнього підписувача та безпосередньо в кваліфікованого надавача електронних довірчих послуг, вимагає відповідної кваліфікації адміністратора реєстрації, а також може застосовувати інші способи первинної ідентифікації за зафіксованими відповідним чином політиками, наприклад: BankID, MobileID, FaceID (ідентифікація за технологією об'ємного розпізнавання обличчя), TouchID або FingerPrintID (ідентифікація за технологією розпізнавання малюнку відбитка пальця (пальців)), SmartID – використання комбінацій наведених вище способів ідентифікації. Доведено основні зміни в організаційно-правових механізмах ЄС забезпечення безпеки надання електронних довірчих послуг.

5. Обґрунтовано необхідність перегляду цілей та завдань міжнародної технічної допомоги, відмовившись від отримання матеріально-технічних засобів у сфері ІТ, які постійно морально й фізично застарівають швидше, ніж всі інші активи, та зорієнтувавшись на отриманні та постійному вдосконаленні необхідних для цифрової економіки знань та навичок широкого загалу населення, запровадженні прозорих та зрозумілих підходів до забезпечення безпеки чутливої для громадян, суспільства та держави інформації, а також на необхідності визначення в Україні своїх пріоритетів у переході до цифрової економіки, які, зокрема, мають співвідноситися з аналогічними цілями в ЄС.

Для організації належної взаємодії з відповідними інституціями Європейського Союзу, взаємного визнання рішень, зокрема, внесення некваліфікованих провайдерів кваліфікованих електронних довірчих послуг до довірчих списків, затвердження схем електронної ідентифікації, роботи з ENISA в розвиток Угоди про асоціацію необхідно розпочати, підготовку міжнародних договорів України саме у цих сферах. Водночас має бути забезпечена тотожність рівня довіри до результатів оцінки відповідності, починаючи з засобів та систем, які використовуються в електронній ідентифікації та наданні кваліфікованих електронних довірчих послуг, та, в подальшому, суб'єктів надання таких послуг, оцінювання цих суб'єктів та наглядового (контролюючого) органу.

6. Вперше здійснено порівняльний аналіз організаційно-правових механізмів державного управління проведенням акредитації КІС для обміну інформацією з обмеженим доступом в Україні та НАТО, надано оцінку рівня їх інтероперабільності, на основі якої обґрунтовано узагальнюючий висновок щодо наявності в Україні засобів КЗІ для різних ступенів обмеження доступу до інформації, які відповідають національному законодавству та політиці безпеки України та можуть бути, після визначення їх конкретних типів, запропоновані стороні НАТО для погодження оброблення інформації НАТО з обмеженим доступом в Україні.

Також доведено, що Адміністрація Держспецзв'язку може самостійно прийняти рішення, поінформувавши сторону НАТО щодо конкретної КІС, яка відповідає законодавству України про оброблення (пересилання, зберігання) в ній інформації з грифом обмеження доступу NATO "CONFIDENTIAL" та NATO

“RESTRICTED”, а для інформації NATO “SECRET” таке рішення Адміністрація Держспецзв’язку має погоджувати з Військовим комітетом НАТО.

Окрім того, обґрунтовано потенціальну інституціональну готовність інших суб’єктів сектору безпеки і оборони України до організації та виконання заходів з акредитації КІС для обміну інформацією з обмеженим доступом з НАТО, насамперед Мінооборони та Генерального штабу Збройних Сил України, Національної гвардії України, МВС, Держприкордонслужби та Держспецзв’язку та інших.

За результатами ретроспективного аналізу щодо формування нормативно-правової бази системи НАТО PKI (NPKI) запропоновано авторську етапізацію її розвитку за критерієм підтвердження відповідності безпеки засобів та процесів, а саме: створення рамкового середовища та інфраструктури, використання під час дослідної експлуатації формально недозволених через незавершеність процедур тестування засобів електронного підпису (1998 –2006 рр.), розвиток інфраструктури, засобів та сервісів з використанням NPKI (2006 –2013 рр.), розвиток інфраструктури та впровадження проєкту використання сервісів NPKI для всеохоплюючого задоволення інформаційних потреб користувачів штаб-квартири НАТО та країн-членів (з 2013 р.).

Здійснено порівняльний аналіз принципів забезпечення безпеки інформації в NPKI з інфраструктурою електронних підписів, відбудованої в ЄС згідно з Регламентом ЄС з електронної ідентифікації та електронних довірчих послуг, який показав їх взаємну узгодженість. Питання директив з безпеки персоналу, фізичної безпеки, безпеки виробництва загалом охоплені законодавством України у сфері охорони державної таємниці та службової інформації. Імплементація в українське законодавство положень директив з питань акредитації КІС вимагає глибокого аналізу існуючої нормативно-правової бази у сфері передачі КІС секретної та службової інформації, визначення підрозділів, на які покладатиметься відповідальність за акредитацію КІС як під час здійснення відповідних оцінок, так і після отримання КІС статусу акредитованої, уточнення функцій і завдань щодо їх взаємодії, розроблення нормативно-правових актів у цій сфері, насамперед щодо надання відповідних функцій Адміністрації Держспецзв’язку повноважень з встановлення порядку акредитації КІС.

7. Розроблено мотиваційні механізми державного регулювання забезпечення безпеки надання електронних довірчих послуг та конкретні напрями державно-приватного партнерства, реалізація яких дозволить, з одного боку, виключити безпосередній контакт регулятора у сфері захисту інформації з бізнес-структурами, з іншого – надасть поштовх у розвитку інфраструктури захисту інформації та стане підґрунтям для вибудовування інфраструктури нового зразка – безпеки інформації. Проаналізовано причини виникнення, існуючий стан справ та пропозиції щодо розвитку сфери підготовки кадрів у галузі захисту інформації та її безпеки.

8. Визначено основні передумови та чинники, що впливають на систему захисту інформації: системоутворюючий елемент гарантування безпеки надання електронних довірчих послуг, а також на підставі проведеного аналізу сформульовано шляхи реформування цієї галузі та розроблено пропозиції до змін законодавства, які забезпечать трансформацію самої парадигми функціонування

системи – від контролю за процесами захисту інформації до оцінки стану її безпеки. Автором запропоновано комплексне рішення щодо внесення змін або розроблення нових законодавчих актів, що не тільки осучаснить підходи до забезпечення безпеки інформації, а й утворить оновлену екосистему забезпечення безпеки інформації в інформаційно-телекомунікаційних системах критичної інфраструктури, наданні державних електронних послуг, запровадить обмін інформацією про загрози для безпеки інформації між уповноваженими суб'єктами взаємодії, для забезпечення належного рівня безпеки інформації в державних органах, підприємствах, установах й організаціях та оцінки його фактичного стану залучати потенціал фахівців їх підрозділів тощо.

9. Розроблено конкретні рекомендації Раді національної безпеки і оборони України, Держспецзв'язку, Міноборони та Генеральному штабу Збройних Сил України, Мінекономрозвитку, Міносвіти, МЗС, Мінцифри та іншим міністерствам та центральним органам виконавчої влади щодо дієвих кроків з удосконалення сфери захисту інформації та її розвитку, а також розвитку власних спроможностей у протидії загрозам для безпеки інформації, забезпеченні безпеки електронних послуг, що ними надаються.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. Мялковський Д.В. Організаційно-правові механізми державного управління міжнародним співробітництвом України у сфері кібербезпеки. *Теорія та практика державного управління*. 2019. № 3(66). С. 216-226.

2. Мялковський Д.В. Організаційно-правові механізми ЄС та України забезпечення безпеки та довіри до електронних послуг. *Вісник Національної академії Державної прикордонної служби України. Серія: державне управління.* 2019. Вип. 3. URL: http://webcache.googleusercontent.com/search?q=cache:bD9SzShflqYJ:periodica.nadpsu.edu.ua/index.php/governance/article/download/295/296/+&cd=1&hl=uk&ct=clnk&gl=ua.

3. Мялковський Д.В. Механізми державного управління оцінкою відповідності засобів, процесів та суб'єктів електронних довірчих послуг в Україні та ЄС. *Економіка та держава: серія державне управління*. 2019. № 4 (12). С. 80-88.

4. Мялковський Д.В. Механізми державного управління акредитацією комунікаційно-інформаційних систем для обміну інформацією з обмеженим доступом між Україною та НАТО / Д.В. Мялковський, А.І. Семенченко. *Збірник наукових праць Національної академії державного управління при Президентові України*. 2019. Вип. 2. С. 73-83.

5. Мялковський Д.В. Стратегічне управління розвитком кіберзахисту критичної інформаційної інфраструктури України / І.Б. Жиляєв, А.І. Семенченко, Д.В. Мялковський, Т.В. Станіславський. *Публічне управління та адміністрування в Україні*. Одеса, 2018. №3. С. 44-51 (в частині пропозицій до визначення об'єктів критичної інфраструктури у сфері телекомунікацій та цифрових послуг).

6. Мялковський Д.В. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної

інфраструктури / А.І. Семенченко, Д.В. Мялковський, Т.В. Станіславський. *Інвестиції: практика та досвід*. Київ, 2018. №18. С. 87-95 (в частині вибору можливих міжнародних стандартів з оцінки, моніторингу та вимірювання ефективності заходів з безпеки інформації).

Статті в зарубіжних виданнях:

7. Mialkovskyi D.V. The overview of procedures for the creation and evaluation of conformity of cryptographic means and cryptosystems in Ukraine. *News of Science and Education*. 2019. № 5(66). P. 38-48.

Опубліковані праці апробаційного характеру

8. Мялковський Д.В. Електронні послуги: стан та актуальні завдання нормативного регулювання задля підвищення довіри до їх результатів. *Науково-практичне забезпечення децентралізації надання послуг в об'єднаних територіальних громадах*: тези доповідей науково-практичної конференції (м. Київ, 18 квітня 2018 р.). Київ: ІПК ДСЗУ, 2018. С. 121-126.

9. Мялковський Д.В., Карташов В.М. Удосконалення українського законодавства у сфері електронних довірчих послуг та безпеки інформації: першочергові кроки. *Сучасні інформаційні технології та кібербезпека*: матеріали науково-практичної конференції (м. Київ, 15-16 листопада 2018 р.). Київ, 2018. С. 81-82.

10. Семенченко А. І., Мялковський Д. В., Станіславський Т. В. Огляд кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури: науково-методологічні підходи до організації та проведення. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України:* тези XI Всеукраїнської науково-практичної конференції (м. Хмельницький, 15 листопада 2018 р.). Хмельницький : Вид-во НАДПСУ, 2018. С. 290-292.

11. Мялковський Д. В. Інноваційні механізми ЄС з підвищення довіри до електронних послуг. *Побудова інформаційного суспільства: ресурси і технології*: матеріали XVIII Міжнародної науково-практичної конференції (м. Київ, 19-20 вересня 2019 р.). Київ, 2019. С. 279-283.

12. Мялковський Д.В., Семенченко А. І. Механізми державного управління акредитацією комунікаційно-інформаційних систем для обміну інформацією НАТО з обмеженим доступом. *Прикладні системи та технології в інформаційному суспільстві:* зб. тез доповідей і наук. повідомл. учасників III Міжнародної науково-практичної конференції (м. Київ, 30 вересня 2019 р.). Київ: Київський нац. ун-т імені Тараса Шевченка, 2019. С. 116-120.

13. Мялковський Д.В. Організаційно-правові механізми ЄС та України забезпечення безпеки та довіри до електронних послуг. *Організаційно-управлінські та психологічні аспекти сучасного ринку праці України:* тези доповідей VIII Всеукраїнської науково-практичної конференції молодих науковців (м. Київ, 29 жовтня 2019 р.). Київ: ІПК ДСЗУ, 2019.С. 130-132.

14. Мялковський Д.В. Оцінка безпеки комунікаційно-інформаційних систем НАТО. *Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання:* матеріали науково-практичної конференції (м. Київ, 19-20 листопада 2019 р.). К.: ІССЗЗІ КПІ ім. Ігоря Сікорського, 2019. С. 226-233.

Опубліковані праці, які додатково відображають наукові результати дисертації

15. Мялковський Д.В. Аналіз предметної області ідентифікації та автентифіікації / Д.В. Мялковський, З.А. Орєшко, О.В. Потій. *Радіотехніка*: всеукраїнський міжвідомчий науково-технічний збірник. Тематичний випуск "Інформаційна безпека". Харків, 2017. №191. С. 120-127.

16. Мялковський Д.В. Алгоритми криптографічного гешування, які застосовуються в сучасних блокчейн-системах / О.О. Кузнецов, Ю.І. Горбенко, В.В. Онопрієнко, І.В. Стельник, Д.В. Мялковський. *Радиотехника*: Всеукр. межвед. науч.-техн. сб. Харьков: ХТУРЕ. 2019. Вып. 198. С. 44-53.

17. Мялковський Д.В. Дослідження алгоритмів криптографічного гешування, які застосовуються в сучасних блокчейн-системах / О.О. Кузнецов, Ю.І. Горбенко, В.В. Онопрієнко, І.В. Стельник. *Радиотехника:* всеукр. межвед. науч.-техн. сб. Харьков: ХТУРЕ. 2019. Вып. 198. С. 54-74.

18. Mialkovskyi D. Code-Based Schemes for Post-Quantum Digital Signatures / Alexandr Kuznetsov, Anastasiia Kiian, Andriy Pushkar'ov, Danylo Mialkovskyi, Oleksii Smirnov, Tetiana Kuznetsova. *IDAACS 2019*: *2019 IEEE 10th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Metz, 18-21 September, 2019). Ecole Nationale d'Ingénieurs de Metz, Université de Lorraine, 2019.

19. Mialkovskyi D. Opportunities to Minimize Hardware and Software Costs for Implementing Boolean Functions in Stream Ciphers / Alexandr Kuznetsov, Oleksandr Potii, Nikolay Poluyanenko, Oleksii Smirnov, Igor Stelnyk, Danylo Mialkovskyi. *International Journal of Computing,* 18(4).

АНОТАЦІЯ

Мялковський Д.В. Державне регулювання забезпеченням безпеки надання електронних довірчих послуг. Рукопис.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. Інститут підготовки кадрів державної служби зайнятості України. Київ, 2020.

У дисертаційній роботі вирішено актуальне наукове завдання розроблення комплексного механізму державного управління забезпеченням безпеки надання електронних послуг.

Доведено необхідність розглядати інфраструктуру електронного підпису як критичну інформаційну інфраструктуру, забезпечуючи її безпеку не тільки з урахуванням як законодавства у сфері захисту інформації та електронних довірчих послуг, а й у сфері кібербезпеки. Обгрунтовано необхідність перегляду цілей, завдань та способів отримання і використання міжнародної технічної допомоги. Визначено необхідність, існуючу спроможність та шляхи розвитку національної системи оцінки відповідності у сфері довірчих послуг та безпеки інформації, продукції, процесів і систем надання електронних послуг.

Досліджено підходи НАТО в забезпеченні безпеки інформації та інформаційно-телекомунікаційних систем, визначено їх сильні сторони, доцільність

та шляхи їх імплементації в Україні. З'ясовано основні передумови та чинники, що впливають на систему захисту інформації в Україні, а також на підставі проведеного аналізу визначено шляхи реформування цієї галузі та розроблено пропозиції до змін законодавства.

Розроблено конкретні рекомендації державним органам щодо дієвих кроків з удосконалення галузі захисту інформації та її розвитку, а також розвитку власних спроможностей у протидії загрозам інформації, забезпеченні її безпеки та довіри до послуг, що ними надаються.

Ключові слова: система захисту інформації, безпека інформації, безпека надання електронної довірчої послуги, кібербезпека, ідентифікація, електронний цифровий підпис, електронні довірчі послуги, оцінка відповідності.

ANNOTATION

Mialkovskyi D.V. The public administration's mechanism for to ensure security in electronic services. Manuscript.

Dissertation for obtaining the scientific degree of The Candidate of Science in Public Administration, by specialty 25.00.02 – Mechanisms of public administration. Ukrainian State Employment Service Training Institute. Kyiv, 2020.

In the dissertation the actual scientific problem of development of the complex mechanism of state management of providing trust in electronic services is solved. The results obtained in the course of the research confirm the achievement of the set goal and the decision of the tasks, give the grounds to formulate such conclusions and practical recommendations.

Discrepancies and gaps in national terminology have been identified and the author's definition of specific terms has been proposed. The analysis of the electronic digital signature models of individual countries with the models of the basic UNCITRAL e-commerce laws and electronic signatures identified their similarities and problems, including interoperability. An analysis was carried out and the possibility of using modern national cryptographic algorithms in the electronic service delivery systems was determined.

The need to consider electronic signature infrastructure as a critical information infrastructure has been proven, ensuring its security not only in the light of both information security and electronic trust services legislation and cybersecurity. The necessity to review the goals, objectives and methods of obtaining and using international technical assistance is justified. Necessity, existing capacity and ways of development of national system of conformity assessment in the field of trust services and security of information, products, processes and systems of provision of electronic services are determined.

NATO's approaches to information security and information and telecommunication systems are explored, their strengths, feasibility and ways to implement them in Ukraine are identified. The basic prerequisites and factors affecting the information security system in Ukraine have been identified, as well as the ways of reforming this sector have been determined and the proposals for legislative changes have been developed.

Specific recommendations to state authorities on effective steps to improve information security and its development, as well as to develop their own capabilities in counteracting threats to information, ensuring its security and trust in the services provided.

Key words: information protection system, information security, trust in electronic services, cybersecurity, identification, electronic digital signature, electronic trust services, conformity assessment.

SOMMAIRE

Réglementation gouvernementale de la sécurité des services de confiance électroniques. Sur les droits du manuscrit.

La thèse de candidat en sciences de l'administration publique sur une spécialité 25.00.02 – mécanismes de l'administration publique. Institut de formation du personnel du Service public de l'emploi de l'Ukraine, Kiev, 2020.

Dans la thèse, la tâche scientifique réelle de développement du mécanisme complexe de la gestion par l'État de la sécurité de la prestation de services électroniques est résolue. Les résultats obtenus au cours de la recherche confirment la réalisation de l'objectif fixé et la solution des tâches, permettent de formuler de conclusions suivantes et recommandations pratiques.

La nécessité est prouvée de considérer l'infrastructure de signature électronique comme une infrastructure d'information critique, garantissant sa sécurité non seulement en tenant compte de la législation dans le domaine de la protection de l'information et des services de confiance électronique, et dans le domaine de la cybersécurité. La nécessité est argumentée de revoir les buts, les objectifs et les méthodes d'obtention et d'utilisation de l'assistance technique internationale. La nécessité, les capacités existantes et les moyens de développement du système national d'évaluation de la conformité dans le domaine des services de confiance et de la sécurité des informations, des produits, des processus et des systèmes de fourniture de services électroniques sont précisées.

Les approches de l'OTAN pour garantir la sécurité de l'information et des systèmes d'information et de télécommunications sont étudiées, leurs forces, leur opportunité et les moyens de leur mise en œuvre en Ukraine sont identifiés. Les principales conditions préalables et facteurs influençant le système de protection de l'information en Ukraine sont déterminés, ainsi que sur la base de l'analyse menée, les moyens de réformer cette branche sont déterminés et des propositions de modifications de la législation sont élaborées.

Des recommandations spécifiques ont été élaborées pour les organes publics sur les mesures efficaces à prendre pour améliorer le domaine de la protection et du développement de l'information, ainsi que le développement de leurs propres capacités pour contrer les menaces informatiques, assurer sa sécurité et sa confiance dans les services qu'ils fournissent.

Mots-clés: système de sécurité de l'information, sécurité de l'information, sécurité du service de confiance électronique, cybe é, identification, signature numérique électronique, services de confiance électronique, évaluation de la conformité.

Підписано до друку 10.07.2020
Формат 148х210 мм. Обл.-вид.арк. 0,9.
Наклад 100 прим.

Свідоцтво серії ДК № 1805 від 25.05.2004
Віддруковано з оригінал-макета в Інституті підготовки кадрів державної служби зайнятості України
03038, м. Київ, вул. Нововокзальна, 17, тел. (044) 536 -14-85